REMARKS

Applicant respectfully requests reconsideration of the present application in view of the foregoing amendments and in view of the reasons that follow.

The specification has been amended to correct minor grammatical and typographical errors. No new matter has been added.

The drawings have been amended to correct a minor typographical error found in Figure 3.

No claims are currently being canceled or added.

Claims 1-63 are currently being amended.

This amendment amends claims in this application. A detailed listing of all claims that are, or were, in the application, irrespective of whether the claims remain under examination in the application, is presented, with an appropriate defined status identifier.

After amending the claims as set forth above, claims 1-63 are now pending in this application.

In the Office Action, claim 58 was objected to because of a typographical error noted in the Office Action. Claim 58 has been amended to correct that minor informality.

In the Office Action, claims 1-5, 8-12, 15-19, 22-26, 29-33, 36-40, 43-47, 50-54 and 57-61 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,606,385 to Aikawa et al.; and claims 6-7, 13-14, 20-21, 27-28, 34-35, 41-42, 48-49, 55-56 and 62-63 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Aikawa et al. in view of U.S. Patent No. 6,175,850 to Ishii et al. These rejections are traversed with respect to the presently pending claims, for at least the reasons given below.

Independent claim 1 has been amended to recite that a control section changes an encrypting operation at a next encrypting stage a plurality of times when it is determined that the encrypting operation at the next encrypting stage should be changed,

wherein the determining section determines whether the intermediate data at the next encrypting stage of the encrypting operation should be changed depending on at least a plurality of random numbers, based on the encrypting stage data at the current encrypting stage from the encrypting operation section,

wherein the encrypting stage data includes the intermediate data at the next encrypting stage, and

wherein the control section changes the intermediate data at the next encrypting stage a plurality of times depending on the plurality of random numbers, in order to cancel an influence of the plurality of random numbers on the encrypting operation.

Support for these added features to presently pending claim 1 may be found, for example, on page 36, lines 8-13, which explains why a plurality of random numbers are used in order to cancel an influence of the random numbers. No such features are believed to be disclosed, taught or suggested by the cited art of record.

Note also that all of the other presently pending independent claims have been amended in a similar manner, and thus these claims are also believed to be patentable over the cited art of record.

The dependent claims are patentable due to their dependencies on one of the presently pending independent claims discussed above, as well as for the specific features recited in those claims.

For example, dependent claim 2 has been amended to recite that the determining section determines whether the intermediate data at the next encrypting stage of the encrypting operation should be changed based on whether or not the current encrypting stage from the encrypting operation section is determined to be a stage to determine a random number conditional branch. Dependent claims 9 and 16 have been amended in a similar manner. Such features are not believed to be disclosed, taught or suggested by the cited art of record.

Accordingly, since there are no other objections or rejections raised in the Office Action, Applicant believes that the present application is now in condition for allowance, and an early indication of allowance is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 19-0741. Should no proper payment be enclosed herewith, as by a check being in the wrong amount, unsigned, post-dated, otherwise improper or informal or even entirely missing, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 19-0741. If any extensions of time are needed for timely acceptance of papers submitted herewith, Applicant hereby petitions for such extension under 37 C.F.R. §1.136 and authorizes payment of any such extensions fees to Deposit Account No. 19-0741.

Respectfully submitted,

June 14, 2004
Date

Phillip J. Articola
Registration No. 38,819

FOLEY & LARDNER LLP
Customer Number: 22428
Telephone: (202) 672-5300
Facsimile: (202) 672-5399

Fig. 3